JIRBDAI

Journal of Institutional Research, Big Data Analytics and Innovation

Nigerian Internet Banking Fraud: A Legal and Cybersecurity Perspective on Emerging Trends and Institutional Vulnerabilities

Egenti, Grace E.

Department of Cybersecurity, National Open University of Nigeria
gegenti@noun.edu.ng;
ORCID: https://orcid.org/0009-0004-8939-0662

ABSTRACT Internet banking has rapidly transformed Nigeria's financial services landscape, but it has also introduced significant cybersecurity risks and exposed critical legal gaps. The financial industry is now grappling with a steep rise in online fraud, driven by weak regulatory enforcement and evolving digital threats. This paper investigates the key legal and cybersecurity challenges contributing to internet banking fraud in Nigeria. Drawing on secondary data from industry reports, academic studies, and reputable media sources, the study employs trend analysis and thematic synthesis to examine patterns in financial loss and fraud occurrence. The findings reveal a sharp increase in cyberattacks, closely linked to outdated IT infrastructure, insufficient multi-factor authentication, insider threats, and regulatory inconsistencies. Compared to institutions in industrialized countries, Nigerian banks demonstrate limited capacity to prevent and respond to fraud. To address this, the study recommends stronger regulatory oversight, targeted investment in cybersecurity infrastructure, and capacity-building for financial and enforcement institutions. These interventions are vital to strengthening digital security, rebuilding public trust, and ensuring the stability of Nigeria's growing digital economy.

KEYWORDS: Cybercrime, Cybersecurity, Financial Sector, Internet Banking Fraud, Nigeria, Regulation

I. INTRODUCTION

As the technological age advances, the disparity in cybersecurity readiness is a significant obstacle, particularly for countries attempting to negotiate the intricacies of a world system that is becoming more interconnected by the day, and although there have been significant advancements as a result of this digital transformation, it has also revealed serious weaknesses in the protection of private information and systems. As threats from hacktivists, cybercriminals, and even state-sponsored actors grow more complex and pervasive, cybersecurity issues within these agencies have become more pressing (Pum, 2025). The multifaceted field of cybersecurity, which includes technology, procedures, and policies, is used to protect data, computer networks, and computer systems (desktops and laptops) against damage, attacks, and unauthorised access (Juneja et al., 2024; Madnick et al., 2024). Attacks on the nation's financial institutions have greatly increased by a whopping 182% higher than what banks in other countries experience (*Rising Cyber Threats Pose Serious Concerns for Financial Stability*, 2024). The Nigeria Inter-Bank Settlement System reported that between 2019 and 2023, bank clients lost at least N59.33 billion as a result of criminals defrauding over 80,658 of them (Temitayo, 2024). Similarly, in July 2023, an account-takeover operation against Guaranty Trust Bank affected over 12,000 customers before it was shut down by the bank's fraud-investigation team (Busola, 2024).

Driven mostly by the arrival of digital payment technology, mobile banking, cryptography and internet banking, Nigeria's financial industry has lately experienced fast digital transformation (Oluwaseun, 2025). With internet penetration increasing and tech-savvy consumers accounting for a growing share of the population, online banking has become rather crucial for Nigeria's economic development. But this digital

VOLUME 1, Issue 3, 2025
https://doi.org/10.5281/zenodo.15700471

transformation has also made banks and their customers more vulnerable to a fresh spectrum of cybersecurity threats and fraudulent activity. Financial system flaws are being used by cybercriminals to commit crimes like Ransomware attacks, fraud, and data theft. Malicious actors find financial institutions appealing because of the high stakes involved in transactions and the enormous volumes of sensitive data they handle, therefore, financial institutions must implement thorough cybersecurity measures in response to these issues (Isaac, 2025). The term cybercrime describes any illegal action carried out via computers and the Internet; this covers anything from stealing millions of monies from internet bank accounts to downloading illicit music, and other fraudulent activities, non-monetary crimes like developing and spreading viruses on other computers or publishing private company data online are also considered cybercrimes (Makeri, 2017). Figures ranging from over 11.6 billion Naira in 2020 to over 52.3 billion Naira in 2024 demonstrate that for the previous several years, financial losses have significantly increased (Reuters, 2025; Premium Times, 2024). This seeming increase in financial losses highlights the need of giving Nigerian banking industry top priority in terms of cybersecurity.

Usually, this issue comes from a basic weakness in computerized banking systems, since banks rely more on internet platforms to allow transactions, they unwittingly raise opportunities for hackers to use security vulnerabilities. Common fraud techniques include phishing, social engineering, malware attacks, and more complex strategies aiming for the human aspect inside financial institutions as well as the technology basis. Empirical studies like those by Olelewe and Onwumere (2024) indicate that rising internet banking fits rather well with rising fraudulent activities. Many instances, legal gaps and inadequate cybersecurity measures worsen these flaws and cause significant financial and reputational damage. Spending on equivalent cybersecurity infrastructure has not matched the phenomenal expansion of digital banking in Nigeria. While banks today offer innovative financial services, thanks to technology, many of the banks still depend on archaic systems and security measures which are unable to keep up with new cyber-threats. These differences in finance and technology not only provide targets for cyber criminals, but also undermine consumers' confidence in the online banking system. With Nigeria most affected, fresh studies show that there is an expected $22 billion cybersecurity budget shortfall all throughout Africa, and with a projected annual damage from cyber events in Nigeria at over $500 million, insufficient security measures obviously have an economic impact (Ogene, 2024).

Moreover, very important in determining the current level of internet banking fraud in Nigeria to be frequent is inadequate application of legislation. Companies like the Nigeria Data Protection Commission (NDPC) and the Central Bank of Nigeria (CBN), whose operations differ, have supported policies aimed to lower cybercrime. For data privacy infractions, for example, the NDPC recently punished some banks; nonetheless, comparable offences are occurring all over the sector (Reuters, 2024). Lack of a clear structure in place to prevent, identify and regulate cyber-attacks makes financial institutions vulnerable targets for cyber criminals, especially with regard to online banking fraud. This paper looks at the several cybersecurity problems influencing the banking system in Nigeria. This study largely addresses the following research issues:

(a). What are the primary cybersecurity vulnerabilities permitting online banking fraud in Nigeria?
(b). How does the quick adoption of online banking affect the rate of fraud within the financial industry?
(c). Which technical and legal weaknesses prevent effective fraud reduction?

This research is vitally crucial since it will enable legislators, financial players, stakeholders and cybersecurity professionals to identify the areas with considerable demand. This study aims to provide useful recommendations for improving cybersecurity systems by means of identification and investigation of the basic components which encourages the increase in online banking fraud. Improved systems help to reduce financial losses; another advantage is increasing consumer confidence and insuring the long-term survival of Nigeria's digital economy.

Using a secondary data analysis technique, this paper references a range of credible sources, such as academic research, industrial studies such as the NIBSS Annual Fraud Landscape (2023), news articles from Reuters and Premium Times, and secondary data analysis approach references. The section on results

VOLUME 1, Issue 3, 2025
https://doi.org/10.5281/zenodo.15700471

emphasizes these tendencies and advances the study by means of so many visualizations including line graphs and bar charts displaying trends in financial losses and event counts.

This study clearly shows how urgently cybersecurity experts, financial institutions, and government officials should synergize to reduce the rising online banking fraud. Improving cybersecurity processes, tightening legislative enforcement, and increasing existing technical investment are the three primary projects to ensure that the needs of the financial sectors are met. Through these projects, Nigeria might provide a strong foundation for a vibrant digital economy and help to lower the risks related to online banking frauds.

Despite regulatory efforts and significant investment in digital platforms, Nigerian financial institutions continue to suffer escalating fraud losses. The root causes span technological vulnerabilities, legal-regulatory gaps, and uneven enforcement capacity. This paper seeks to:

(a). quantify the recent rise in digital fraud within Nigeria's banking sector;

(b). critically assess the effectiveness of existing legal and regulatory frameworks; and

(c). propose a targeted set of policy, technical, and capacity-building interventions.

The remainder of the paper is organized as follows. Section II reviews recent academic and industry literature on fraud-technology interaction. Section III examines Nigeria's legal frameworks and enforcement challenges. Section IV analyzes case-studies and enforcement data. Section V puts forward actionable recommendations, and Section VI concludes with implications and future research directions.

II. LITERATURE REVIEW

To contextualize Nigeria's fraud landscape, we compare three streams of research in Table 1.

Table 1: Overview of Research Streams in Nigeria's fraud landscape

S/N	Study	Focus	Key Finding	Consensus/Disputes
1	Olelewe & Onwumere (2024)	Digital fraud typologies	Increasing use of SIM-swap and malware kits	Converges on technology-enabled identity theft
2	Pandey (2025)	AI-enabled fraud detection	Early AI models reduce false positives by 30 %	Diverges on the role of supervised vs. unsupervised learning
3	Bouveret (2018)	Customer behaviour and fraud	Customers' poor cybersecurity hygiene	Converges on education as key mitigation

Critical Synthesis

(a). **Convergence:** All three studies underscore that evolving attack vectors (e.g., malware, social engineering) exploit both technological and human vulnerabilities.

(b). **Divergence:** While Bouveret (2018) emphasizes user education, Pandey (2025) argues for algorithmic sophistication—highlighting a tension between preventive and detective controls.

Recent work has further refined our understanding of emerging threats. Reis et al. (2024) document AI-driven deep-fake scams; Madnick et al. (2024) analyze cloud-API vulnerabilities; and Onatuyeh et al. (2025) measure the efficacy of multi-factor authentication (MFA) rollouts in West Africa. For example, in August 2024, the Nigerian Data Protection Commission (NDPC) fined Fidelity Bank ₦555 million for failure to report large-scale data breech offenses - a striking illustration of regulatory enforcement gaps (Camillus, 2024). Nigeria's overall fraud-loss rate stood at 5 % of net transaction value in 2023, compared with 2 % across ASEAN-member banks (Bolu, 2024), underscoring a need for regionally tailored

VOLUME 1, Issue 3, 2025
https://doi.org/10.5281/zenodo.15700471

interventions. Given the global proliferation of digital banking, research on cybersecurity within the banking sector has become a primary emphasis. This literature review analyses both local and global perspectives on cybersecurity issues, particularly focusing on online banking fraud in Nigeria.

A. Global Cybersecurity Trends in the Financial Sector

The financial sector is particularly susceptible to hacking activities globally (Bouveret, 2018). Due to swift technological advancements, researchers currently see that cybercrime is evolving at an unprecedented rate (Pandey, 2025). Common threats include phishing, malware, Ransomware, and insider attacks. Research indicates that hackers commonly infiltrate financial networks through various sophisticated techniques, relying on both technology vulnerabilities and human errors. Olelewe & Onwumere (2024) says that phishing is still the main way that attackers get people to give up private information by sending fake emails or websites that look real. Malware and Ransomware attacks are becoming more common as cyber criminals use malicious software to encrypt important data and demand money for the release. The growing number of cyber-attacks around the world shows how important strong security measures and working together across borders are to reduce these risks.

B. Cybersecurity Challenges in Nigeria's Financial Sector

Apart from the great development in digital banking products, online banking fraud has exploded Nigeria. Industry data like the NIBSS Annual Fraud Landscape (2020 - 2024) shows that over the past few years financial aggregate fraud losses in Nigeria rose from ₦15 billion in 2020 to over ₦67.5 billion in 202 - a 350 % increase driven largely by remote-banking exploits clearly showing that losses due to fraud have escalated; recent news stories highlight this Reuters (2025), and in the year 2020, losses went from over N11.6 billion Naira to almost N52.3 billion Naira in the year 2024. This exponential rise points to serious issues with the digital infrastructure in Nigeria. The studies revealed a few things: one was that there is a clear link between the rise in internet banking and the number of frauds. Based on statistics from 2008 to 2019, Olelewe and Onwumere (2024) carried out an empirical study; it is found that higher frequency of simulated events exactly matches with the rising online banking consumption. While there are clearly advantages, the researchers opined that faster digitisation of financial institutions has also increased cybercrime opportunities. The paper underlines how poor cybersecurity policies, including obsolete IT infrastructure and ineffective multi-factor authentication systems allow businesses to remain open to cyber-attacks.

C. Technological Vulnerabilities and Cyber Threats

Many researches have underlined the technology flaws causing vulnerability of Nigerian financial institutions. According to the literature, many Nigerian banks run on obsolete or insufficiently modern systems. Phishing, SQL injections, and denial-of- service (DOS) attacks help hackers to quickly exploit vulnerabilities in this technology difference. For example, Library, (2024) showed various organizations still suffer breaches from the use of old applications and/or systems unable to resist current cyber-attacks. Insider attacks (Sharma, 2023) are also rather significant; employees who have access to sensitive data could either deliberately or inadvertently compromise security by not following best practices. Many cybersecurity experts believe that adding modern technologies like artificial intelligence (AI),chine learning (ML) and cloud computing would help find and lower cyber vulnerabilities (Ogene, 2024). These technologies enable banks be better ready for attacks by means of automated systems that detect threats before it occurs or as soon as they manifest. Emerging research also caution though, that when institutions apply these technologies, attackers are as likely to leverage AI-driven technology to increase the sophistication of their attacks. Thus, even if advances in technology help strengthen defenses, they also introduce fresh complexity that has to be properly regulated. For instance, AI can improve cybersecurity by automating threat detection and response, there are hazards associated with it since cyber criminals

VOLUME 1, Issue 3, 2025
https://doi.org/10.5281/zenodo.15700471

engage it more frequently to automate and launch attacks (Pandey, 2025). Concerns about data sovereignty and dependence on third party companies are two additional security issues brought forth by the increasing use of cloud computing technologies (Ogene, 2024). Thus, choosing trustworthy cloud providers and making sure cybersecurity regulations are followed are crucial to reducing these threats.

D. Regulatory Frameworks and Enforcement Gaps

Furthermore, quite importantly is the regulatory landscape of cybersecurity in Nigeria. Though laws aimed to lower cybercrimes are created by the Nigeria Data Protection Commission (NDPC) and the Central Bank of Nigeria (CBN), their execution is not uniform. Reuters (2024) claims that a bank was fined for data privacy violations brought by illegal personal data collecting; however, the bank stated that it did not violate any law because there was no data breach, and that it did not complete the account opening process for the unnamed customer, whose complaint triggered NDPC's investigation.. Although, this signals a step towards responsibility, comparable violations continue to occur in the sector suggesting that present regulations might not be sufficiently stringent or consistently implemented. Many academics have attacked the disjointed approach of the Nigerian regulatory structure. The literature claims that although many regulations focus primarily on the banking sector, several crucial sectors remain under-regulated in terms of cybersecurity. Notable also is the difference between policy development and execution; according to Ogene, (2024), Cybersecurity incidences in Nigeria is predicted to result in $500 million in losses annually, affecting both the economy and public confidence (Onatuyeh et al., 2025). The results show that in order to reduce these risks, it is essential to invest in emerging technologies, train qualified staff with the necessary skillset, and good governance. So, Nigeria has a large budget deficit, which is estimated at almost $22 billion for cybersecurity across Africa. This investment disparity even more weakens the national general cybersecurity posture.

E. Economic Impacts of Cybersecurity Investment Gaps

Security issues within the banking sector carry significant financial repercussions. In addition to immediate monetary losses, widely reported fraud cases have demonstrated the capacity to undermine customer trust and tarnish the reputations of financial institutions. The rise in fraud losses identified in the NIBSS research (2023) underscores the potential impact of escalating cyber-attacks on the stability of the financial system. Alleged cybersecurity problems make companies and people wary to interact completely with digital financial systems, therefore hindering economic growth and creativity. Moreover underlined in the report is the importance of a basic challenge: insufficient funding for infrastructure supporting cybersecurity. Again, Ogene (2024) noted that the clear financial gap in cybersecurity is a systemic issue whereby financial institutions would be unable to or reluctant to spend money to update their defenses. Apart from defining attack targets, this lack of investment generates a broader economic crisis since reduced client confidence limits the general expansion of the digital economy.

F. Comparative Analysis: Nigeria and Other Regions

Comparative studies have been conducted to place Nigeria's cybersecurity issues in a larger context. Although rich countries have always used creative technologies and strict laws (Lubua & Pretorius, 2019), however, developing countries, for example, Nigeria, have difficulties in these spheres. Global cybersecurity trends show that banks in developed countries usually guarantee more investments in IT infrastructure, comprehensive staff training programs, and strict regulatory control. Nigerian banks frequently face resource constraints and inadequate regulatory cooperation, making them increasingly susceptible to cybercrime (Isaac, 2025; Reis et al., 2024). This gap underscores the imperative to address both technological and regulatory deficiencies in Nigeria while incorporating best practices from other regions. Nigerian institutions can improve their digital infrastructure by implementing international standards and collaborating with global cybersecurity experts (He et al., 2021).

VOLUME 1, Issue 3, 2025
https://doi.org/10.5281/zenodo.15700471

G. Synthesis of Key Findings

The literature points up some recurring themes:

(a). Technological Vulnerabilities: Cybercriminals target Nigerian banks most specifically as antiquated systems and poor application of advanced cybersecurity processes expose these banks.

(b). Inadequate Regulatory Enforcement: Although regulatory frameworks are provided by CBN and NDPR, enforcement is still uneven. There are little consequences for banks that disregard cybersecurity regulations, which lessen the motivation to give security first priority.

(c). Economic Impact: Nigeria's banking industry is rife with cybersecurity threats that jeopardise the institutions' financial soundness, declining customers' confidence, and the instability of the national economy. Significant financial losses, reputational damage, fines from the government, and interruptions in banking activities are all possible outcomes of cyber-attacks.

(d). Comparative Insight: The problems Nigeria tackles highlight the benefits of applying international best practices since they are more relevant in connection with more technologically developed and controlled countries.

These results provide a strong basis for understanding the difficult problems related to internet banking fraud in Nigeria. The approach used to investigate these issues will be described in this article together with thorough findings and suggestions for raising cybersecurity requirements in Nigerian banking sector.

III. METHODOLOGY

The cybersecurity issues and online banking fraud in Nigeria's financial industry are investigated in this paper using the secondary data analysis technique. The study proposes to provide a detailed knowledge of the patterns and components behind the fast upsurge in financial losses by combining data from a variety of reliable sources to guarantee a strong analysis. Sources include industry publications, academic journals, and news items. Industry papers include the NIBSS Annual Fraud Landscape 2023 offer comprehensive numbers on fraud incidents and financial losses suffered by Nigerian banks in recent years. Establishing numerical benchmarks and knowing general trends depend on these studies. Furthermore, scholarly research provides empirical data linking the growth of digital banking to rising fraudulent activity. For instance, the 2024 Olelewe and Onwumere study uses an Auto Regressive Distributed Lag (ARDL) model covering data from 2008 to 2019, therefore proving a notable positive association between the increase in internet banking and fraud incidences. The data collecting strategy consists of a methodical assessment of published works accessible via scholarly databases and internet resources. Keywords such as 'cybersecurity challenges in Nigeria', 'online banking fraud in Nigeria', 'NIBSS fraud report', and 'internet banking and fraud', helped to guide a thorough literature search. While current industry data came from reputable news websites and government reports, databases including ResearchGate, JSTOR, and Google Scholar were quite helpful in locating pertinent academic papers. To guarantee the accuracy of the data, the study comprised just sources judged reliable, current, and directly relevant to the Nigerian financial situation, while discarding the irrelevancies.

Organizing and collecting important quantitative and qualitative data came next once the relevant data were collected. Figures on financial losses, the frequency of fraud incidents, and historical trends were among the quantitative data. Discussions on legislative flaws, technology vulnerabilities, and the financial consequences of cybersecurity investment gaps produced the qualitative materials. This methodical technique made it possible to compare several sources and historical periods, therefore strengthening the validity of the conclusions of this research endeavor. Two complementing components define data analysis for this work; initially, a trend study was done to track the development of fraud incidents and related financial losses. Tracking developments from 2019 to 2024 using time series analysis reveals notable patterns in both the number of fraud cases and the financial losses suffered by Nigerian banks. With help from the ARDL model results of Olelewe and Onwumere (2024), correlation analysis investigates the

VOLUME 1, Issue 3, 2025
https://doi.org/10.5281/zenodo.15700471

relationship between the fast adoption of internet banking and the growth in fraud events. Later in the study, line graphs and bar charts help to clearly show these tendencies from this quantitative research.

Second, a thematic study of qualitative data was done to identify recurrent themes about cybersecurity vulnerabilities, regulatory enforcement flaws, and the wider economic influence of these issues. Data coding was done in order to find trends including obsolete IT infrastructure, insufficient multi-factor authentication, and poor cybersecurity expenditure. The study creates a coherent story that clarifies the fundamental reasons of the growing fraud rates by combining these issues with the quantitative trends. The debate and the later suggestions for improving cybersecurity policies in Nigeria's financial industry are built upon this story.

Though this method has certain advantages, several constraints should be mentioned; sometimes inconsistent reporting standards and definitions found in secondary data from several sources compromised the comparability of the data. Furthermore, some of the scholarly research applied in the study spans prior eras (like 2008-2023) and may not entirely reflect the most current patterns, especially as new trends and patterns are being used by cybercriminals to perpetrate modern attacks. These studies, however, offer the required basis for comprehending the development of cybersecurity issues in the Nigerian context. Furthermore, since the study depend just on secondary data; it could not reflect the complex operational reality or developing patterns that are found in main data collecting techniques, such as interviews with cybersecurity specialists or practitioners.

In terms of ethical issues, this study makes use of publically accessible secondary data and so no further ethical clearance was needed. Still, all sources are painstakingly referenced to uphold data veracity and intellectual integrity. To investigate the cybersecurity issues and online banking fraud in Nigeria, this section on methodologies generally presents a methodical approach combining quantitative trend analysis with qualitative theme research. Combining information from reliable news sources, scholarly studies, and industry reports helps the study to provide a strong and all-encompassing knowledge of the components causing fraud, or exposing banks to vulnerabilities. This strategy finally helps the creation of practical suggestions to improve regulatory enforcement and cybersecurity systems in Nigerian financial sector.

IV. RESULTS AND DISCUSSION

This section provides a comprehensive analysis of online banking fraud in Nigeria using quantitative data, qualitative observations, and comparative perspectives. Our study comprises several sections: trends in financial losses and incident frequencies; the impact of internet banking proliferation on fraud occurrences; the identification of significant cybersecurity vulnerabilities; a comparative analysis between Nigerian banks and those in developed economies; and qualitative insights highlighting the operational challenges encountered by financial institutions.

A. Legal Frameworks and Challenges

Landmark Prosecutions. Since the Cybercrimes Act 2015, two pivotal cases illustrate enforcement trajectories:

(a). 2022 Kano Insider-Fraud Case: Three bank employees were convicted for manipulating transaction logs; evidence preservation difficulties led to a suspended sentence.

(b). 2021 Lagos Cross-Border Phishing Ring: International cooperation with INTERPOL resulted in extradition of key suspects, but cloud-hosted data jurisdictionality delayed trial by 18 months.

B. Legal and Regulatory Gaps

(a). Mutual Legal Assistance: Absence of formalized treaties hampers timely cross-border data sharing.

(b). Digital Evidence Standards: Nigerian courts lack codified guidelines on admissibility and chain-of-custody for forensic artifacts.

(c). Jurisdictional Ambiguities: Cloud-hosted transaction records often fall outside Nigerian territorial reach, complicating prosecution.

VOLUME 1, Issue 3, 2025
https://doi.org/10.5281/zenodo.15700471

C. Enforcement Capacity

A 2023 NDIC survey reveals that only 40 % of EFCC cyber-crime investigators have formal digital-forensics training, and less than 30 % of Federal High Court judges have attended specialized cyber-law workshops - highlighting a critical skills gap.

D. Fraud Trends and Financial Losses

Recent data from industry publications, like the NIBSS Annual Fraud Landscape (2023), articles from Reuters (2025) and Premium Times (2024), indicates a rapid increase in losses due to online banking frauds. Specifically, financial losses in the Nigerian banking sector escalated from about N11.6 billion Naira in 2020 to around N52.3 Billion Naira in 2024. This practically 350% rise in four years highlights not just the growing frequency of incidents but also the growing complexities and degrees of individual and collective fraud cases. Moreover, the frequencies y of fraud incidents has showed interesting increase as well. Reports state that 44,947 fraud incidents were recorded in 2019; by 2023 this figure has increased to over 95,620. These numbers suggest that the frequency of fraud as well as the financial impact of every incidence have been rising over the years. Figure 3 shows the attempted fraud amount between 2022 and 2023; NIBS (Ummah, 2019) recorded that the total attempted and actual loss between 2022 and 2023 significantly increased by 20% and 24% respectively. Also, the first quarter (Q1) of 2022 and 2023 recorded the highest attempted value loss for the respective year. However, Q1 (2023) had a 3% increase when compared with Q1 (2022).

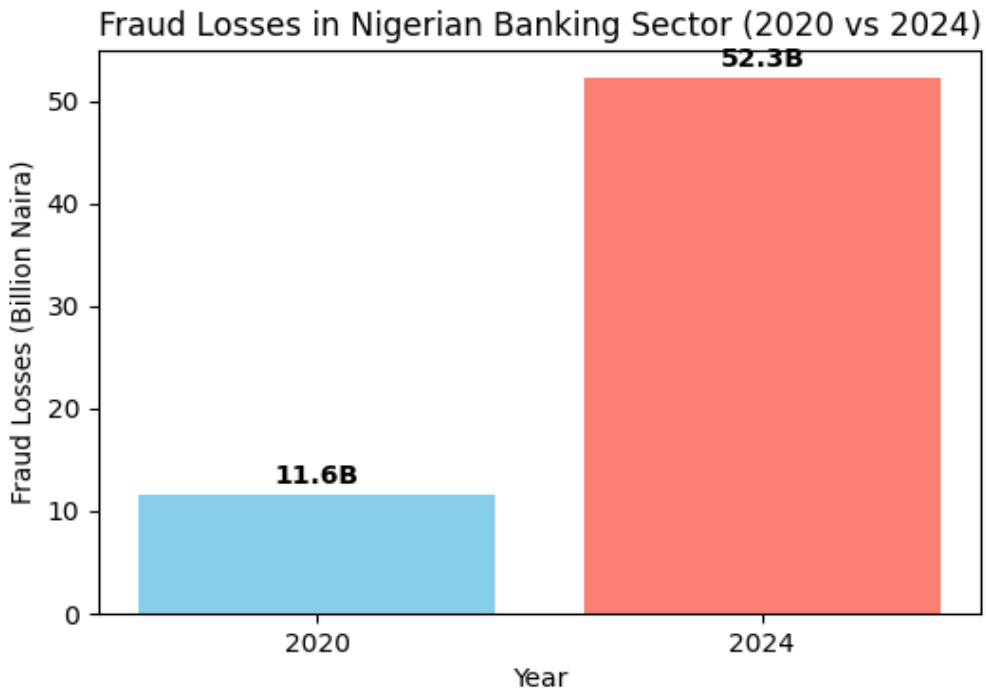

Figure 1: Bar Chart of Fraud Losses (2020 vs. 2024)

VOLUME 1, Issue 3, 2025
https://doi.org/10.5281/zenodo.15700471

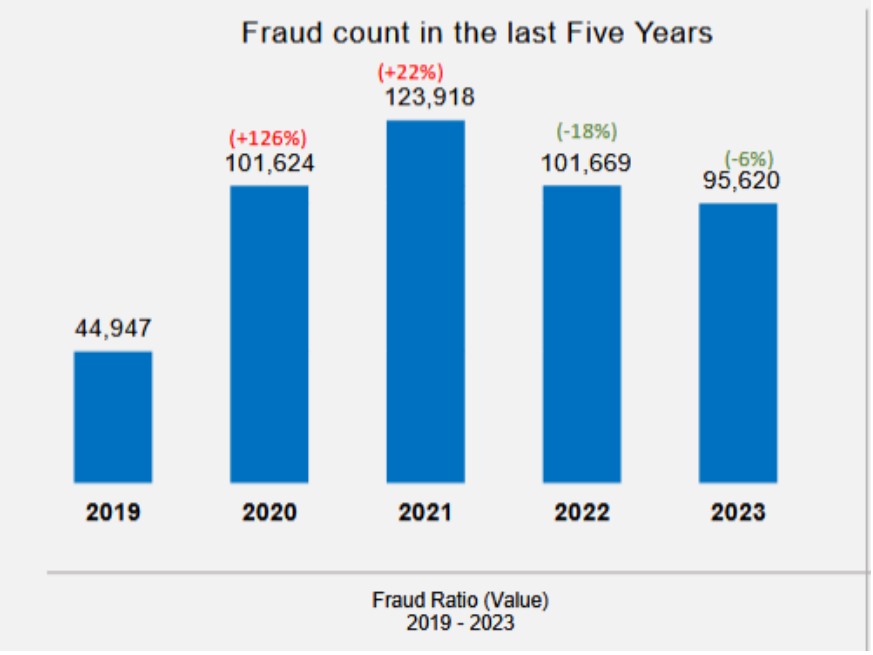

Figure 2: *Bar Chart of Annual Fraud Incidents (2019 vs. 2023)* (Ummah, 2019)

Figures 1 and 2 graphically illustrate these rising trends. Figure 1 illustrates the notable rise in financial losses; Figure 2 clearly indicates the incidence of fraud cases significantly rising. Collectively, they provide a quantitative basis for evaluating the degree of the problem in the Nigerian banking industry.

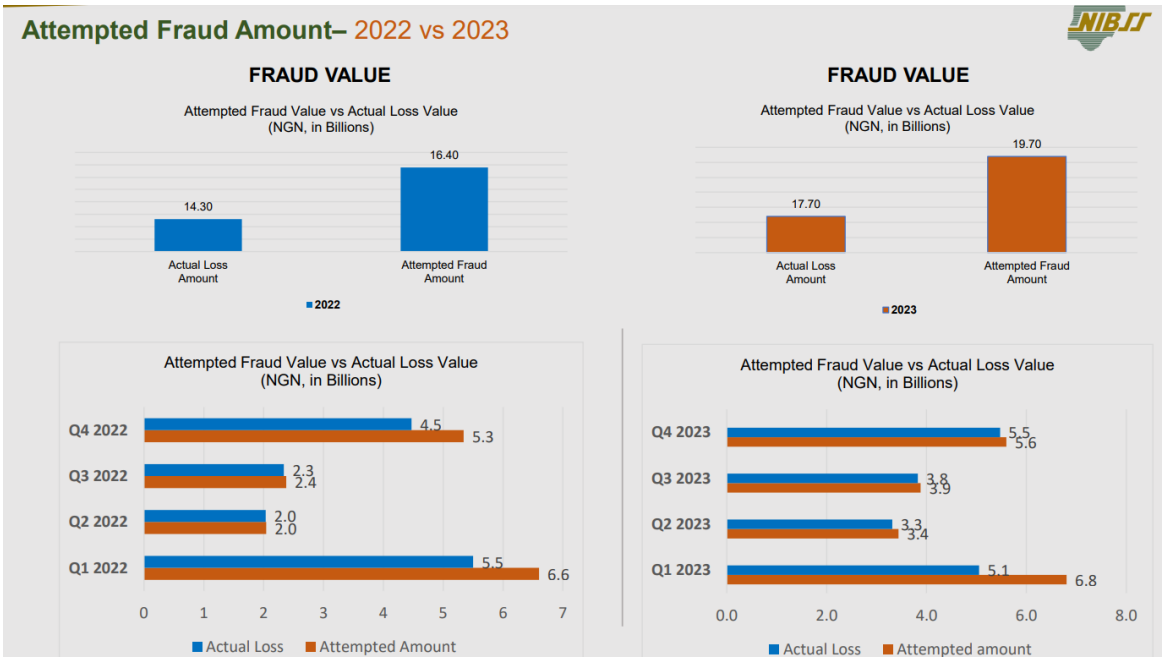

Figure 3: NIBSS Annual Fraud Landscape 2023 (Jan 01, 2023 - Dec 31, 2023)

VOLUME 1, Issue 3, 2025
https://doi.org/10.5281/zenodo.15700471

E. Impact of Internet Banking on Fraud

Our study primarily examines the explicit correlation between the prevalence of fraud and the expansion of internet banking. Olelewe and Onwumere (2024) assert that the increased provision of digital services by Nigerian banks correlates with a heightened propensity for unethical conduct. Their study of 2008 to 2019 using an Auto Regressive Distributed Lag (ARDL) model amply showed a correlation between rising fraud rates and online banking activity. Thus, even if financial inclusion and comfort are being pushed, the speedy digitisation of banking services simultaneously increases the attack surface accessible for hackers. A scatter plot has been generated with approximated data to help characterise this relationship. Even in cases when comprehensive transaction volume data is not publicly available, industry trends and professional opinions helped to predict. On the X-axis, Figure 4 displays expected online banking transaction volumes (in millions) together with matching fraud incidents. Plot fitted linear regression line shows a positive link, therefore confirming the notion that greater fraud possibilities result from higher digital banking activity.

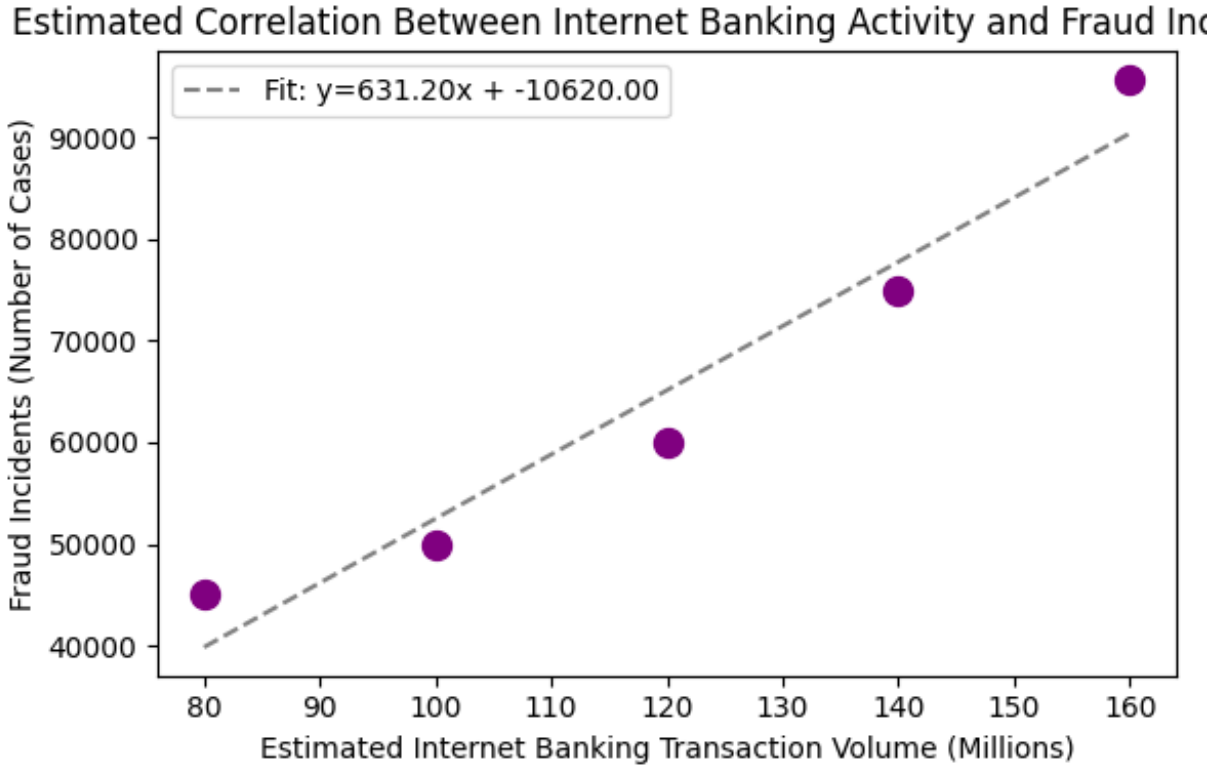

Figure 4: Scatter Plot Illustrating Estimated Correlation between Internet Banking Transaction Volume and Fraud Incidents

The expected data provide a good substitute for understanding this relationship. The good trend indicates, however, that the expanding digital banking industry in Nigeria demands for concurrent improvements in cybersecurity rules to reduce the accompanying risks, even if evolving.

F. Cybersecurity Vulnerability

The research also reveals a range of cybersecurity weaknesses supporting the increased online banking fraud risk. The technical and legal shortcomings in Nigerian banking institutions are a recurring topic in the literature. Two identified vulnerabilities are:

VOLUME 1, Issue 3, 2025
https://doi.org/10.5281/zenodo.15700471

(a). Outdated IT Infrastructure: Many banks still run on old, non-regularly maintained legacy systems that permit modern attackers to exploit them. Using outdated hardware and software increases banks' vulnerability to be unable to identify or counter advanced threats by cybercriminals.
(b). Insufficient Multi-Factor Authentication (MFA): Weak or poorly implemented MFA systems allow cybercriminals easy access to consumer accounts, therefore compromising data integrity of customers. Strong authentication techniques are a good way to maintain integrity in online financial systems.
(c). Insider Threats: Banking cybersecurity vulnerabilities are much exacerbated by human factors such as staff ignorance or criminal intent. Insider threats, whether intentional or accidental, could lead to illegal exposure of private information, therefore escalating the risk.
(d). Regulatory Gaps: Although policies to prevent cyber-threats have been established by the Nigeria Data Protection Commission (NDPC) and the Central Bank of Nigeria (CBN), their actual implementation differs. This division of regulatory authority offers opportunities for fraudsters to exploit system vulnerabilities.
(e). Lack of skilled personnel: The limited number of qualified cybersecurity personnel is a significant weakness in Nigeria's cybersecurity resilience, especially in the banking system, or the reliance on international cybersecurity firms, who might not adequately handle or understand Nigeria-specific threats, has resulted from a lack of indigenous experience.
(f). Funding Challenges: The substantial investment needed to repair security holes throughout the continent is demonstrated by the estimated $22 billion cybersecurity budget shortfall for Africa. Cyber incidents in Nigeria are predicted to cause $500 million in losses annually as a result of poor expenditures in cybersecurity infrastructure (Ogene, 2024).

Figure 5 presents a graphical representation that theoretically highlights these shortcomings and how they increase the general cybersecurity risk and a rising cybersecurity threat.

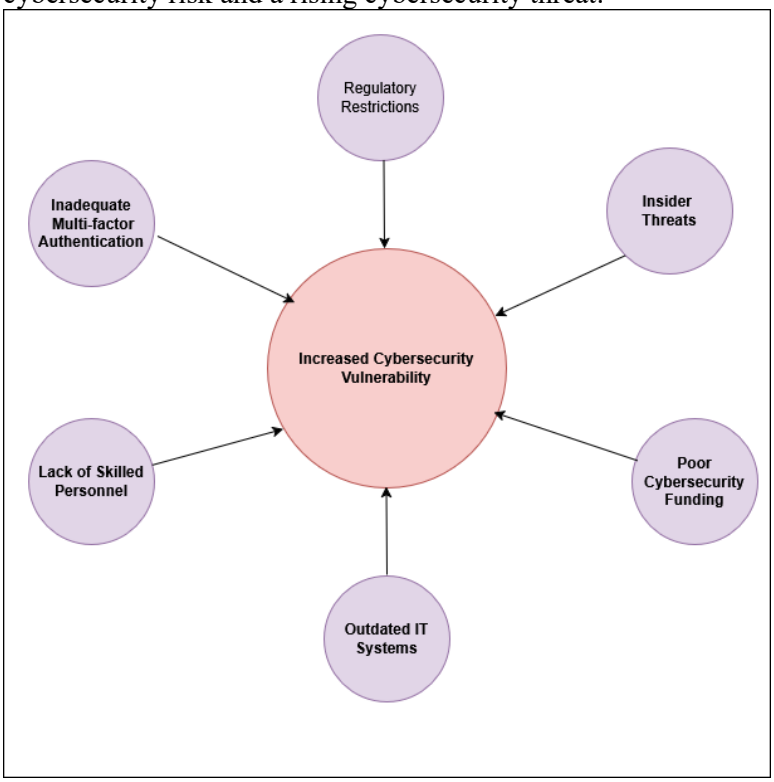

Figure 5: Graphical representation illustrating Key Cybersecurity Vulnerabilities

VOLUME 1, Issue 3, 2025
https://doi.org/10.5281/zenodo.15700471

G. Comparative Analysis: Nigerian Banks vs. Developed Economies

Problems within the banking system bring to highlight the fact that Nigerian banks have more problems than banks in other rich countries. Established banks in developed countries have used IT infrastructure, strict implementation of rules, investments in cybersecurity, and technical acceptance. When done together, these steps make it less likely that hackers will thrive. Nigerian banks could run with obsolete systems, little resources, and inconsistent implementation of policies. They are more likely to come across major and consistent fraud incidents. Table 2 compares the rich country institutions notable areas of cybersecurity investment and procedures with Nigerian banks. This table displays variations in the quality of IT infrastructure, the strictness of rules, the amount of money spent on cybersecurity, and the rate at which new technologies are adopted. The difference makes it even more important for Nigerian financial institutions to follow best practices around the world and put more money into current cybersecurity solutions.

Table 2: Comparative Table or Chart Summarizing Cybersecurity Investment and Practices between Nigerian Banks and Banks in Developed Economies

Features	Nigerian Banks	Banks in Developed Countries
IT Infrastructure	• Often outdated • Limited modernisation	• Regularly updated with advanced technology
Regulatory Enforcement	• Inconsistent • Fragmented enforcement	• Strict, comprehensive and consistently applied
Cybersecurity Investment	• Lower Investment • Significant Funding Gap (approximately $22B)	• Higher investment with robust cybersecurity budgets
Technology Adoption	• Slower integration of AI/ML threat detection	• Rapid adoption of advanced cybersecurity tools

H. Qualitative Insights and Case Examples

Quantitative trends are much strengthened by case studies already available in publication and qualitative opinions from corporate leaders. Examining regulatory data and consulting financial professionals reveal that many Nigerian institutions appear to be struggling with operations, which generates security concerns. Several bank executives have noted, for example, that the primary issues requiring solutions to maintain strong cybersecurity defenses are limited funding and the challenge of modernizing existing systems. Sometimes phishing is an issue; which involve using phoney websites that resemble actual bank websites, fraudsters routinely persuade victims to provide private information. Though banks still find it difficult to completely safeguard consumer accounts, more and more consumers are realising how crucial it is to have secure multi-factor login systems. One major issue remains is the insider attacks. Particularly in cases without sufficient full-coverage monitoring systems, even well-trained employees could unintentionally bypass security systems and architectures. These qualitative findings reveal that technical errors are exacerbated by human and regulatory elements, therefore generating a complex and always changing hazardous environment. Knowing people in the sector makes it abundantly evident that Nigerian banking systems must have a comprehensive plan including not only improved technology but also better application of rules and continuous personnel training.

I. Synthesis of Findings

Based on the statistics (NIBSS, 2025), Nigerian online banking presents many issues. Modern days fraud is a more difficult problem. From 44,947 incidents in 2019 to 95,620 in 2023; from N11.6 billion Naira in 2020 to over N52.3 Billion Naira in 2024; financial losses grew (Premium Times, 2024). This suggests that

VOLUME 1, Issue 3, 2025
https://doi.org/10.5281/zenodo.15700471

the threat is getting more real. Second, as it offers hackers quick access to digital data, several studies show that the growth of internet banking is closely related with a surge in fraud (The Guardian Nigeria, 2024). This is still important even if internet banking raises the GDP. Among the several cybersecurity issues demanding attention are regulatory restrictions, outdated IT systems, inadequate multi-factor authentication, insider threats, and so on (Daily Trust, 2024). Furthermore, shown by the data are poor resources, outdated technologies, and unequal regulatory compliance which led Nigerian financial institutions to be ranked as less than those of industrialized nations (Independent Magazine Nigeria 2024). These findings highlight immediately the requirement of minor changes. These should address growing cybersecurity costs, infrastructure modernizing, and more regulatory control and implementation.

This report presents a whole picture of the problems affecting Nigeria's digital banking sector by the use of both personal observations and quantitative data. Figures 1–5 reinforces the argument that, absent significant improvements, persistent trends in online banking fraud would continue eroding Nigeria's customers' confidence and financial stability (Lorna, 2025). They also draw attention to certain inclinations. Nigerian online banking fraud demands legislation, human problems, and technology. Nigeria's digital banking system is seriously underdeveloped as financial losses and cases climb from N11.6 Billion Naira in 2020 to over N52.3 Billion in 2024. The synthesized results are linked to the literature and investigated with respect to policy, technology, and practice. Given regularity, it is quite compelling that online banking fraud is growing even more significant. Data shows that as digital banking becomes more prevalent, criminals are utilizing loopholes to pilfers significant volumes. Publications that serve to represent this propensity include Premium Times (2024), Reuters (2025), and the NIBSS Annual Fraud Landscape (2023). The unexpected rise in financial losses and incidents suggests that cybercriminals are focusing more at specific accounts and honing their methods on a daily basis. This escalation highlights the need for banks to look at and enhancing cybersecurity measures as a matter of urgency.

Olelewe and Onwumere (2024) claimed that the growth of internet banking greatly increases fraud. Using digital banking increases exploitation as more people do. Our expected scatter plot (Figure 4) shows positive correlation between fraud and internet banking volume. Though the data presented is approximations based on public trends and professional opinions, the pattern supports the qualitative awareness that digital development without cybersecurity spending increases the attack surface of cybercriminals. This problem stems from technological faults; as many Nigerian banks still in possession of obsolete IT systems which lacks contemporary digital security. Older infrastructure permits hackers to easily get around security mechanisms. Based on research on cybersecurity vulnerabilities, weak multi-factor authentication and lack of cybersecurity training increase this challenge. . Even a sophisticated system can be compromised by staff ineptitude or hostility. Apart from flaws in regulatory enforcement, these psychological and technical components enable cybercriminals to operate easily and seamlessly free from constraints.

The Nigerian regulatory environment has improved cybersecurity even if enforcement is not uniform. The NDPC fined a Nigerian bank for data security breaches, therefore reaffirming banks' accountability (Reuters, 2024). Similar breaches are still documented, suggesting that sector-wide policies may not be enough. Ogene (2024) studies on cybersecurity and IT governance show that the $22 billion cybersecurity budget shortage of Africa aggravates enforcement problems. The difference between policy creation and execution leaves many banks vulnerable, which fuels fraud and fraudulent practices. This paper also highlighted Nigerian banks versus those of developed nations. Mention was made of how investments in cybersecurity tools, IT infrastructure, and stricter IT infrastructure laws benefits developed-region banks. These banks have less financial losses despite high digital transaction volumes because they have stronger cyber threat identification, prevention strategies, and high response rate. Fraud is more common and costly for Nigerian institutions with little resources and obsolete tools. The comparative table (Table 1) shows these differences once more underlining the benefits of global best practices. Improved cybersecurity investment and consistent regulations could close this gap for Nigerian financial institutions, so boosting operational resilience and customer confidence.

VOLUME 1, Issue 3, 2025
https://doi.org/10.5281/zenodo.15700471

These conclusions have major financial implications; apart from financial losses, fraud and cybersecurity issues erode consumer confidence, a basic component of a functional financial system. Customers are less inclined to use digital banking services if they feel their personal data or money is at risk, so hindering the growth of the digital economy. Years of customer loyalty and market competitiveness could be influenced by damage to bank reputation brought about by well reported fraud incidents. The research claims that falling trust may impede economic development, therefore influencing the stability of the national economy.

Qualitative perspectives of view of industry professionals improve numerical trends. Banking executives most usually mention cybersecurity issues as obsolete system updates, operational sloppiness, and financial restrictions. These operational issues draw attention to how institutional resistance or a dearth of competent experts can prevent the implementation of new technologies. Other social engineering methods and phishing campaigns expose insufficient technical solutions. To reduce these risks, a full strategy must call for staff training and customer awareness efforts. These figures demonstrate that Nigeria needs a different reaction to internet banking fraud. Key areas of concerns are IT system updates and artificial intelligence/machine learning threat detection. Still, much-needed are better cybersecurity funding and regulatory enforcement. Banks have to be proactive in order to safeguard their assets and re-establish customer trust in digital banking.

Professionals in government authorities, financial institutions, and cybersecurity professionals must work together. Policy proposals should fix legal loopholes by enforcing regulations and guiding institutions towards expenditures in cybersecurity infrastructure. Projects in capacity-building teaching consumers on cybersecurity best practices and bank employees on cybersecurity best practices help to reduce human errors generating fraud, because digital banking is very important for Nigeria's economy and for Nigerians. While online banking has numerous benefits, the current trend of increasing fraud and losses cannot be sustained. One has to combine legislation, technology, control, and training into a comprehensive approach. Without such attention, the vulnerability of Nigerian banks could restrict public confidence in the digital economy and slow down progress.

V. CONCLUSION AND RECOMMENDATION

This study has shown that Nigeria's digital-fraud losses ballooned by 350 % between 2020 and 2024, driven principally by legacy-system vulnerabilities and uneven enforcement capacity. Our critical review of existing legal frameworks reveals structural gaps in mutual assistance, digital-evidence standards, and jurisdiction over cloud data. By quantifying these linkages and benchmarking against regional peers, we contribute a novel, data-driven understanding of Nigeria's fraud ecosystem. This paper emphasizes the need of Nigeria's banking system addressing the problem of fraud aiming at monetary theft via online banking. Secondary data showed that fraud has considerably heightened in frequency and financial influence in recent years. From 2020 to 2024, fraud cases almost quadruple; the financial losses almost triple. These incidents underline the diminishing integrity of Nigerian internet banking systems and the growing complexity of hacking. This study found a notable relationship between the rise in fraud and the more people utilizing internet banking. Criminals seize the higher transaction volumes as more people engage in digital banking. To do this, some banks still use outdated IT systems, inadequate multi-factor authentication, and other system vulnerabilities. This suggests that illegal activities have been made possible by digitization of banking, so weakening the security protection improvement. Figure 4 shows the expected results compatible with this positive correlation. The research found major security flaws that increased the online banking fraud risk. Included are obsolete IT systems, poor multi-factor authentication mechanisms, insider threats, and unsolved legal issues. The graphical representation in Figure 5 helps to explain these challenges; yet, the comparison study in Table 1 shows that, in terms of technical investments and regulatory compliance, Nigerian banks fall short of those of industrialized countries.

These flaws greatly raise costs, and apart from the obvious financial losses, consumers are growing more reluctant to rely on digital banking systems as they are always vulnerable. People may limit their usage of

VOLUME 1, Issue 3, 2025
https://doi.org/10.5281/zenodo.15700471

digital financial instruments if they feel their personal data and money are under risk. This would hinder economic growth, sustainability and innovation. Moreover, dishonest people that attract a lot of media attention destroy reputation, hence, over an extended period; this could compromise the market stability and economy of Nigeria.

These risks call for immediate reduction using different ways; to enable the quick identification and resolution of problems, Nigerian banks should adopt the use of current IT infrastructure and engage in investing modern security technologies, such as artificial intelligence and machine learning as top priority. Second, organizations such as the Nigeria Data Protection Commission and the Central Bank of Nigeria have to carefully review current laws, create stricter rules, and follow-up implementation procedures to help to reduce hacking incidents, and fraudulent practices. Thirdly, major initiatives to enhance public education and training programmes are absolutely essential for teaching consumers and bank staff on spotting and stopping fraud and fraudulent activities.

Nigeria's attempt to digitize its banking system has both significant benefits and somewhat negative consequences. Nigerian banks have to swiftly and methodically solve cybersecurity challenges, strengthen policies, and enhance public education; else, they would keep compromising financial stability and economic development. Working with cybersecurity experts is one way to improve these results and provide more improvements in the banking system. The cooperation among the government, financial institutions, and cybersecurity experts will improve consumer confidence and boost the protection of Nigeria's digital economy.

RECOMMENDATION

(a). For Policymakers

i. CBN MFA Guidelines (0–6 months): Issue mandatory guidelines on MFA implementation for all banks.
ii. Mutual Legal Assistance Protocol (6–12 months): Negotiate MLATs with top five correspondent-bank jurisdictions.
iii. Digital Evidence Act (12–18 months): Enact statutory standards for forensic admissibility.

(b). For Banks and FinTechs

i. Annual Training Grant: Allocate at least ₦2 billion per year (via CBN) for IT-staff certification in digital forensics and incident response.
ii. AI-Driven Early-Warning Systems: Deploy supervised-learning models to flag anomalous transactions, with quarterly performance reviews.
iii. Customer Awareness Campaigns: Partner with NCC and NDIC to run bi-annual cybersecurity workshops for retail customers.

(c). For Law Enforcement and Judiciary

i. EFCC Cyber-Unit Expansion: Double staffing and provide advanced forensic labs within 12 months.
ii. Judicial Cyber-Law Workshops: Mandate annual cyber-law continuing legal education (CLE) for all Federal High Court judges.
iii. Specialised Cyber-Fraud Task Force: Establish a joint EFCC-CBN task force to coordinate real-time information-sharing and rapid-response drills.

As a call to Action, we urge coordinated reforms - spanning policy, technology, and capacity building - to arrest the rising tide of digital fraud. We recommend (1) conducting an in-depth qualitative interviews with bank cybersecurity practitioners, and (2) developing and field-testing AI-driven early-warning models calibrated to Nigeria’s transaction-volume profiles.

REFERENCES

VOLUME 1, Issue 3, 2025
https://doi.org/10.5281/zenodo.15700471

[1.] Bolu A. (2024, July 4). "₦82.4 billion: Top 5 hacks and fraud cases in Nigeria between 2023 and 2024". techpoint.africa. [https://techpoint.africa/insight/major-hack-and-fraud-cases-in-nigeria/]
[2.] Busola A. (2024, August 15). "'Customers' data not affected' — GTB says hackers tried to compromise website". The Cable News [https://www.thecable.ng/customers-data-not-affected-gtb-says-hackers-tried-to-compromise-website/]
[3.] Bouveret, A. (2018). Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment. *IMF Working Papers*, *18*(143), 1. https://doi.org/10.5089/9781484360750.001
[4.] Camillus E. (2024, August 22) "Nigerian data agency fines Fidelity Bank for breaches". The Reuters. [https://www.reuters.com/business/finance/nigerian-data-agency-fines-fidelity-bank-breaches-2024-08-22]
[5.] He, Y., Aliyu, A., Evans, M., & Luo, C. (2021). *Correction : Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19 : Scoping Review Corresponding Author : 23*, 29877. https://doi.org/10.2196/29877
[6.] Isaac, O. (2025). *Evaluating Cybersecurity Risks in Nigeria ' s Commercial Banking Sector : An Empirical Analysis*. *February*.
[7.] Juneja, A., Goswami, S. S., & Mondal, S. (2024). Cyber Security and Digital Economy: Opportunities, Growth and Challenges. *Journal of Technology Innovations and Energy*, *3*(2), 1–22. https://doi.org/10.56556/jtie.v3i2.907
[8.] Library, B. (2024). Learning Lessons from the Cyber-Attack British Library cyber incident review. March, 4–8.
[9.] Lorna, L. (2025). Cybersecurity Challenges in Nigeria ' s Government Agencies and Ministries. February.
[10.] Lubua, E. W., & Pretorius, P. (2019). *Cyber-security Policy Framework and Procedural Compliance in Public Organisations*. *August*.
[11.] Madnick, B., Huang, K., & Madnick, S. (2024). The evolution of global cybersecurity norms in the digital age: A longitudinal study of the cybersecurity norm development process. *Information Security Journal*, *33*(3), 204–225. https://doi.org/10.1080/19393555.2023.2201482
[12.] Makeri, Y. A. (2017). Cyber Security Issues in Nigeria and Challenges. *International Journal of Advanced Research in Computer Science and Software Engineering*, *7*(4), 315–321. https://doi.org/10.23956/ijarcsse/v6i12/01204
[13.] Ogene, F. (2024). *Cybersecurity and IT Governance Challenges in Nigeria : Strategic Investment Needs and the Path Forward for a Resilient Digital Economy*. *186*(55), 41–46.
[14.] Olelewe, C. A., & Onwumere, J. U. (2024). The Impact of Internet Banking on Bank Fraud in Nigeria. Asian Journal of Economics, Business and Accounting, 24(5), 510–524. https://doi.org/10.9734/AJEBA/2024/v24i51326
[15.] Oluwaseun, F. (2025). *Emerging Cyber Threats in Nigeria : A Deep Dive into Future Risks*. *July 2022*.
[16.] Onatuyeh, E. A., Oghorodi, D., Okpako, E. A., Ojei, E., Osakwe, G., Chinedu, N. B., Okoh, S. K., Odu, V. C., Chinedu, P. U., & Nwankwo, W. (2025). Cybersecurity and Business Survival in Nigeria: Building Customer'S Trust. *African Journal of Applied Research*, *11*(1), 786–813. https://doi.org/10.26437/ajar.v11i1.882
[17.] Pandey, M. P. (2025). *Sachetas Cybercrime in the Digital Era : Impacts , Awareness , And Strategic Solutions for a Secure Future Sachetas*. *4*(1), 32–37.
[18.] Pandey, P. (2025, February). AI-Enabled Multi-Factor Authentication (MFA) Systems for Private and Public Cloud Security. In *2025 International Conference on Electronics and Renewable Systems (ICEARS)* (pp. 886-889). IEEE.
[19.] Pum, M. (2025). *Cybersecurity Challenges in Nigeria ' s Government Agencies and*

VOLUME 1, Issue 3, 2025
https://doi.org/10.5281/zenodo.15700471

Ministries. *February*.

a. *Rising Cyber Threats Pose Serious Concerns for Financial Stability*. (2024, April 9). IMF. https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability

[20.] Reis, O., Oliha, J. S., Osasona, F., Obi, O. C., Researcher, I., Researcher, I., Water, S., & Researcher, I. (2024). *Cybersecurity Dynamics in Nigerian Banking : 5*(2), 336–364. https://doi.org/10.51594/csitrj.v5i2.761

[21.] Sharma, A. (2023). *ISSN : 2320-5407 Manuscript Info Abstract Chapter 1 : Introduction : - ISSN : 2320-5407 Objectives : -*. *12*(10), 10–25. https://doi.org/10.21474/IJAR01/19614

[22.] Temitayo J. (2024, November 21). "Nigerian banks face 182% more weekly attacks than global counterparts". BussinessDay [https://businessday.ng/news/article/nigerian-banks-face-182-more-weekly-attacks-than-global-counterparts/]

[23.] Ummah, M. S. (2019). No 主観的健康感を中心とした在宅高齢者における 健康関連指標に関する共分散構造分析Title. *Sustainability (Switzerland)*, *11*(1), 1–14. http://scioteca.caf.com/bitstream/handle/123456789/1091/RED2017-Eng-8ene.pdf?sequence=12&isAllowed=y%0Ahttp://dx.doi.org/10.1016/j.regsciurbeco.2008.06.005%0Ahttps://www.researchgate.net/publication/305320484_SISTEM_PEMBETUNGAN_TERPUSAT_STRATEGI_MELESTARI

VOLUME 1, Issue 3, 2025
https://doi.org/10.5281/zenodo.15700471